part of #7



**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

In re Application of: Timothy E. Dickson
Serial No. 09/494,897
Filed: January 31, 2000
For: **FRAUD DETECTION THROUGH FLOW RATE ANALYSIS**

Examiner: Von Buhr, Maria N.
Art Unit: 2125

Commissioner for Patents
Washington, D.C. 20231



Sir:

**DECLARATION UNDER RULE 37 CFR 1.131**

I hereby declare that:

1. I am currently employed by Gilbarco Inc. and hold the title of Vice President of Engineering.

2. I am the inventor of the invention disclosed and claimed in U.S. Patent Application Serial Number 09/494,897, entitled **FRAUD DETECTION THROUGH FLOW RATE ANALYSIS**, which was filed January 31, 2000.

3. Upon review of my records, I remember conceiving the present invention while traveling to a meeting in late February 1999. The meeting, and therefore conception of the present invention, is evidenced by an email (Exhibit A) that I received on February 18, 1999.

4. At least as early as April 21, 1999, I was in possession of the present invention as is evidenced by the Patent Memoranda (PM) 9914 (Exhibit B). Specifically, the second and fourth bullet points of the Patent Memo illustrate the concept of the present invention to a degree sufficient for one of ordinary skill in the art to practice the invention.

5. I submitted PM 9914 to Steven Terranova, an in-house patent attorney at Gilbarco, on or about April 21, 1999.

6. After submitting PM 9914 to Steven Terranova, PM 9914 was scheduled for a patent committee meeting at Gilbarco, which was routinely held once per month. Pursuant to policies then in place, and to the best of my recollection, I discussed the invention disclosure with Steven Terranova in May 1999 to explain the contents of PM 9914.

7. I submitted a supplement PM 9914 (Exhibit C) to Steven Terranova on or about July 1, 1999.

8. To the best of my recollection, I presented PM 9914 at the Gilbarco Patent Committee meeting in June 1999 for consideration. During this meeting, I was questioned by the Gilbarco Patent Committee members about the technical aspects of my invention. I am also a member of the Gilbarco Patent Committee and was so in July 1999.

9. On or about December 3, 1999, I received a copy of the draft of the patent application from the law firm of Coats and Bennett, PLLC from Steven Terranova, who at this time was employed by the law firm of Coats and Bennett, PLLC.

10. In December 1999 and early January 2000, I reviewed the draft of the patent application for my invention described in PM 9914, made comments and observations, and sent back such to Steven Terranova for consideration. Shortly thereafter I received a revised draft patent application for my review which incorporated my comments and observations.

11. On January 31, 2000, the application containing the invention described in PM 9914 was filed with the United States Patent and Trademark Office by Coats and Bennett, PLLC. I receive a copy of the patent application as filed at the United States Patent and Trademark Office by Coats and Bennett, PLLC.

12. I hereby acknowledge that willful false statements and the like are punishable by fine or imprisonment, or both (18 U.S.C. § 1001), and may jeopardize the validity of the application or any patent issuing thereon. All statements made herein are true and made on information and belief are believed to be true.

Timothy E. Dickson 1/8/03

Timothy E. Dickson Date

Exhibit A

## Taylor M. Davenport

**From:** Steve Terranova [sterranova@withrowterranova.com]
**Sent:** Monday, December 16, 2002 4:51 PM
**To:** Tmd
**Subject:** FW: Changes to ISO 9564

-----Original Message-----
From: Dickson, Tim [mailto:Tim.Dickson@gilbarco.com]
Sent: Monday, December 16, 2002 4:42 PM
To: Terranova, Steve
Subject: FW: Changes to ISO 9564

Steve

The very last line of Carl's message refers to the meeting "next week". This is the ANSI meeting that I was on a plane to (or from) when I wrote the original patent notes and fleshed out the idea. This pins it down to sometime at the end of Feb, likely on or before Feb. 26 (a Friday).

> -----Original Message-----
> From: Dickson, Tim
> Sent: Friday, February 19, 1999 7:19 AM
> To: Carl Campbell; Dennis G. Abraham; Azita Amini; Rich Ankney; Tim
> Dickson; Jim Foti; Rick Hite; Darlene Kargel; Rick Kastner; Ken
> Keirnan; Beth Lynn; Ralph Poore; John Pratt; Gerry Scott; John Sheets;
> Rena Smith; John Spence; Stuart Taylor
> Cc: Whitley, Chris; Marion, Ken; Jackson, Peter; Charles Heckman;
> Cynthia Marion; Eileen Roehrig; Jeff Hallman; Ken Ringeman; Phil Robertson
> Subject: RE: Changes to ISO 9564
>
> Carl
>
> Your message (I think) points out that the recommendation to use
> double length master keys and single length session keys in X9.24 was
> flawed and probably should be rescinded. Are you suggesting that the
> use of double length PIN encryption keys should be recommended in its
> place? You do not address DUKPT, which does not currently call for
> double length PIN encryption. If this is still considered acceptable
> (until the advent of AES), why not just withdraw the recommendation
> for double length master keys in X9.24 and mandate that DUKPT be used.
> This would simplify things a great deal and help get systems based on
> single length master keys (many without unique key per
> terminal) out of the field much more quickly. It would also be
> consistent with direction coming from the major payment systems and
> would cost a small fraction (<10%) of the amount it would take to put
> unique, double length "fixed keys" in place. Deployment of double
> length "fixed keys" in the U.S. retail market would not cost millions,
> it would cost billions. The cost to retail petroleum alone would be a
> billion dollars.
>
> With that kind of cost barrier there are several things that could
> happen, none of them good. First, companies may do nothing until AES
> is available, since every recommendation sites that as the real goal.
> Even if they decide to implement, the staggering cost will delay and
> prolong deployment as they try to stretch the cost over several fiscal
> years. Also, the use of double length "fixed" keys, puts a premium on
> soundly designed physical security and unique key per terminal. This
> will result in higher equipment prices and longer development cycles
> (6-18 months) to provide suitable equipment. Companies already

> changing to DUKPT (and they are) will be very unlikely to stop in
> mid-deployment and start over, nor will they immediately repeat that
> expenditure by deploying new double length key equipment when it is
> finally available. Lastly, this kind of expenditure would virtually
> guarantee the delay of AES deployment by 5-10 years.
>
> As the security advisors to the retail financial industry, I believe
> X9F3 must provide clear direction that is both economically sound and
> can feasibly be followed prior to the availability of AES. Double
> length "fixed" keys do not seem to meet any of these criteria. If
> DUKPT is still considered adequate security, I urge the group to make
> a clear statement to the retail financial industry which can be loudly
> endorsed by the major switches and payments systems.
>
> Tim
>
> -----Original Message-----
> From: Carl Campbell [SMTP:Carl_Campbell@compuserve.com]
> Sent: Thursday, February 18, 1999 2:40 PM
> To: Dennis G. Abraham; Azita Amini; Rich Ankney; Tim Dickson; Jim Foti;
> Rick Hite; Darlene Kargel; Rick Kastner; Ken Keirnan; Beth Lynn; Ralph
> Poore; John Pratt; Gerry Scott; John Sheets; Rena Smith; John Spence;
> Stuart Taylor
> Subject: Changes to ISO 9564
>
> Date: February 18, 1999
>
> To: X9F3-R
>
> From: Carl Campbell (610-353-8747)
>
> Subject: Changes to ISO 9564
>
>
> As you probably know by now, the January meeting of ISO 68-6-6
> significantly revised 9564. Perhaps the most significant change was
> to mandate the use of double-length keys for PIN-encryption, a change
> with which I fully concurred, but one which some in the U.S. may find
> unduly stringent.
>
> X9.24 has already been changed to mandate double-length keys for
> key-encrypting keys, though the current (ballot) version of X9.24
> would presumably allow single-length keys to be used for
> PIN-encryption, provided these keys are replaced fairly frequently.
> There is very much of a risk that, without the concurrent change to IS
> 9564, some U.S. organizations might implement systems that would use
> the master-key-session-key technique
> with double-length master keys (key-encrypting keys) but single-length
> session keys (PIN-encryption keys). Such an implementation would, in my
> opinion, be a very serious mistake.
>
> First, it would be costly to change the current key-management
> infrastructure to use double-length keys. Second, it will soon become
> cost-effective to exhaustively determine a PIN-encryption key that is
> used for only a few transactions. Thus many millions could be spent
> introducing a system that will, itself, become obsolete in a few
> years.
>
> Rather than use the master-key-session-key technique with
> double-length master keys, it seems very much better to use a
> double-length key as the actual PIN-encryption key, and never change
> this key unless its physical compromise is suspected. The one slight
> disadvantage to using the same
> (double-length) key for extended periods (e.g. years) is the "PIN
> guessing"
> attack discussed in R-TDEA.DOC (in the X9F3 February '99 distribution).
> However the introduction of Format-3 into 9564 provides a way to prevent

> this attack. Furthermore, as also discussed in R-DTEA.DOC, eliminating
> the
> need for key down-line-loading can allow the existing single-DES
> infrastructure to be used for triple-DES, in such a way that single-DES
> and
> triple-DES devices can operate concurrently and transparently on the same
> system, the only required changes being to the new PIN-entry devices and
> to
> host security modules. Since there are no apparent benefits to periodic
> key changes for double-length keys, the use of fixed, double-length
> PIN-encryption keys appears to be the simplest and most secure alternative
> to the current single-DES approach.
>
> As indicated above, a third PIN-block format has been added to IS
> 9564. It therefore seemed desirable to have a paper that compares
> them. An initial version of such a paper is attached. However it is
> not intended for widespread distribution, since it outlines the
> details of certain fraud scenarios.
>
> Thanks very much. I hope to be at next week's meeting, and see many
> of you there. Have a safe trip!
>
> Carl << File: C:\Pbfcom2.doc >>

Exhibit B

9914

April 21, 1999

Patent Memo – Fraud detection through inference

Problem – Fraud against liquid measuring devices that consists of a replacement of some portion of the device with a modified part of parts is becoming more prevalent and the attackers more sophisticated. This increases the difficulty of preventing/detecting fraud since the mechanisms responsible for that detection/prevention are often the mechanisms which are modified or replaced.

This increase in fraud results in larger and larger consumer losses, increasing cost of devices as anti-fraud mechanisms (usually mechanical) are added and a decrease in consumer confidence.

Solution – Provide a software based method of inferential fraud detection that does not depend on any fraud detection in the liquid measuring device itself. This technique would use a number of methods to infer potential fraud and alert appropriate individuals or authorities. Successfully countering one of the methods would not disable the fraud detection capability.

The approach would be to use normal system activity to spot abnormal activity that might indicate fraud. It depends on the fact that fraud will continue over a long time in order to get pay back for the effort and cost to introduce the fraud in the first place.

Since most gasoline retailing operations employ a central controller, that controller would be the focal point for data gathering, data analysis, and device/module authentication used in this multi-layer fraud detection scheme. Alternatively, data analysis could be done off site. This scheme could be used in addition to any fraud detection/prevention mechanisms in the liquid measuring device itself.

The fraud detection system could include, but not be limited to the following:

- Authentication of the dispensers software to detect modification. This can be done by a number of techniques already in the industry, such as use of cryptographic signatures.

- Monitoring and analysis of the vapor returned at a station or group of stations. Based on the level of efficiency of the vapor systems the amount of vapor returned on non-fraudulent fuel sales should significantly higher than fraudulent transactions.
- Monitoring of flow rates. The rate per gallon on average over all non-fraudulent transactions should significantly higher than the flow rate exhibited during fraudulent sales. This would be determined by a comparison of the avg. flow rate versus the volume delivered. For example, if a non-fraudulent fuel sale of 10 gal. is delivered at an avg. of 8 gal. per minute, a fraudulent fuel sale of 8 gal. (but presented the consumer at 10 gal.) should exhibit a marked lower avg. flow rate, up to 20%).
- A similar or additional approach could be to measure the time of the fuel delivery at each fueling position and watch for a change or consistently faster time per gal. indicating a fraudulent device.
- Monitor for increases or decreases in flow rate at a dispenser which do not match the overall pattern for the rest of the dispensers at the site.
- Contrast Tank Monitor (or even probe data) measurements against volume reported dispensed by the liquid measuring device whenever that device is the sole device in operation.
- Preload a set of norms for a station of like configuration that is know to contain now fraudulent data. This data can then be used to compare against the equipment on that site.
- In order to guard against a site in which all units are modified in the same manner at the same time. Data collected could be sent to a central location that is used to compare that site's data against either a control data set or a large number of sites.
  - Lack of data from any site would also indicate a potential fraud situation.

Exhibit C

To: Steve Terranova
From: Tim Dickson

Patent Memo - Fraud detection through inference
Additional information added 7/1/99

Problem - Fraud against liquid measuring devices that consists of a replacement of some portion of the device with a modified part of parts is becoming more prevalent and the attackers more sophisticated. This increases the difficulty of preventing/detecting fraud since the mechanisms responsible for that detection/prevention are often the mechanisms which are modified or replaced.

This increase in fraud results in larger and larger consumer losses, increasing cost of devices as anti-fraud mechanisms (usually mechanical) are added and a decrease in consumer confidence.

Solution - Provide a software based method of inferential fraud detection that does not depend on any fraud detection in the liquid measuring device itself. This technique would use a number of methods to infer potential fraud and alert appropriate individuals or authorities. Successfully countering one of the methods would not disable the fraud detection capability.

This methodology has been used successfully by the credit card industry to detect fraud in credit card usage at the point of sale.

The general approach would be to use normal system activity or a reference model to spot abnormal activity that might indicate fraud. It depends on the fact that fraud will continue over a long time in order to get pay back for the effort and cost to introduce the fraud in the first place, thus producing a statistically significant signature. Something similar has been done in the tank monitor arena to use operational statistics gathered over time to indicate potential leaks.

Since most gasoline retailing operations employ a central controller, that controller would be the focal point for data gathering, data analysis, and device/module authentication used in this multi-layer fraud detection

scheme. Alternatively, data analysis could be done off site. Most of the data referenced here is already available in retail petroleum systems or could be easily made available to populate the statistical models. This scheme could be used in addition to any fraud detection/prevention mechanisms in the liquid measuring device itself.

The fraud detection system could include, but not be limited to the following:

1. Authentication of the dispensers software to detect modification. This can be done by a number of techniques already in the industry, such as use of cryptographic signatures. The metrologically significant portions of the software in the dispenser could be cryptographically signed such that if modified the correct signature could not be returned to an on-site, or off-site, monitoring device upon request.

2. Monitoring and analysis of the vapor returned at a station or group of stations. Based on the level of efficiency of the vapor systems the amount of vapor returned on non-fraudulent fuel sales should significantly higher than fraudulent transactions. Detection of this would require measuring the amount of vapor returned per gallon displayed to the consumer. This value should be relatively constant during non-fraudulent deliveries. If the amount of vapor being returned dipped significantly it would indicate either a problem with the vapor system or potential fraudulent activate where the dispenser was delivering less volume to the consumer than was being displayed on the dispener.

   Monitoring more than one station would provide a larger database and make it possible to more accurately discriminate potential fraudulent activity from normal variations in the vapor system or vapor systems operating incorrectly.

3. Monitoring of flow rates. The rate per gallon on average over all non-fraudulent transactions should significantly higher than the flow rate exhibited during fraudulent sales. This would be determined by a comparison of the avg. flow rate versus the volume delivered. For example, if a non-fraudulent fuel sale of 10 gal. is delivered at an avg. of

8 gal. per minute, a fraudulent fuel sale of 8 gal. (but presented the consumer at 10 gal.) should exhibit a marked faster avg. flow rate, up to 20%). The flow rate, gallons delivered /time of delivery = avg. flow rate, should remain relatively constant for any given dispenser.

4. A similar or additional approach could be to measure the time of the fuel delivery at each fueling position and watch for a change or consistently faster time per gal. indicating a fraudulent device.

   A sudden increase in the average flow rate either from transaction to transaction or for extended periods would indicate potential fraud, especially if a unit capable of 10 GPM max. suddenly is delivering 12.5 GPM which would be the result of the calculation in a situation where the dispenser has been modified to deliver only 8 gallons while displaying 10 to the consumer.

   One embodiment would be to have the time variable of the calculation supplied by the station controller making it very difficult to prevent detection of the change in rate of delivery.

5. Monitor for increases or decreases in flow rate at a dispenser which do not match the overall pattern for the rest of the dispensers at the site. If only one, or several, of the dispensers at the site are being operated in a fraudulent manner, their pattern of operation will be different when compared to the other dispensers, of the same model, on the site.

6. Contrast Tank Monitor (or even probe data) measurements against volume reported dispensed by the liquid measuring device whenever that device is the sole device in operation. When a single pump is delivering, the accuracy level of current tank monitors is such that even the occurrence of a single "short delivery" of 20% may be detectable for a 10 or 15 gallon deliver.

7. Preload a set of norms for a station of like configuration that is know to contain now fraudulent data. This data can then be used to compare